INFORMATION SECURITY POLICY OF UAB EPSO-G GROUP OF COMPANIES

OBJECTIVE	To establish the key information security objectives of the Group, management principles, and responsibilities, ensuring the ongoing suitability and compliance of the information security management system with the Group's strategic objectives, its effectiveness and continuity in accordance with operational, legal, regulatory, and contractual requirements.
SCOPE OF APPLICATION	For all Group companies

1. Terms and abbreviations used

1.1. The terms and abbreviations used in this policy have the following meanings:

Company	UAB EPSO-G (legal entity code 302826889), AB Amber Grid (legal entity code 303090867), UAB TETAS (legal entity code 300513148), Energy cells, UAB (legal entity code 305689545), LITGRID AB (legal entity code 302564383), BALTPOOL UAB (legal entity code 302464881) or UAB EPSO-G Invest (legal entity code 306949519).
Group information	Any form of data managed by the Group (any Company), regardless of the method of recording or transmission (stored in documents, photographs, computer disks, portable electronic and other information storage media, drawings, sketches, diagrams, and any other means of information (data) storage (retention), as well as in verbal form, i.e., existing in human memory and not stored (expressed) in any material form).
Information security	Ensuring the confidentiality, availability, integrity, and authenticity of information.
Information Security Management System (ISMS)	The Group applies a risk-based management system aimed at creating, implementing, managing, monitoring, evaluating, supervising, and improving information security. The ISMS consists of: organizational structure, planning, responsibilities, internal regulations, and assets. The ISMS is implemented in all Companies and covers all their divisions, Employees, and Third Parties to the extent that they may influence Information Security.
Information security incident	An event that threatens the availability, authenticity, integrity, or confidentiality of the Group's information, data, or services provided or accessible through network and information systems.

Information Assets	Group information, software, hardware, services and infrastructure assets necessary for the functioning of information technology and telecommunications.
Information Asset Manager (Owner)	An employee appointed by management in accordance with the procedure established in the internal legal acts implementing the Policy, responsible for the security of Information Assets or specific categories (types) thereof, controlling access to these Information Assets.
Sensitive information	The Group information that is not classified as Public Information (e.g., information for internal use, confidential or commercial (production) secrets, information not disclosed to the public, personal data).
Third parties	All persons who are not Employees or members of the Companies' collegial bodies. Third parties also include persons undergoing practical training at any of the Companies.
Management	A group of managers consisting of the Company's CEO and top-level managers who report directly to the CEO.
Public information	The Group information that is publicly disclosed or may be disclosed in cases and in accordance with the procedure established by law (e.g., general contact information, areas of activity, services provided, press releases, news, job advertisements, publicly disclosed reports and notifications to stock exchanges, announcements of tenders, etc.). The procedure for opening data, approved by Order No 4-1150 of the Minister of Economy and Innovation of the Republic of Lithuania of 28 December 2020 "On the Approval of the Procedure for Opening Data".

1.2. The terms, as defined in Annex 1 to the corporate governance policy of UAB EPSO-G Group of Companies "List of terms used in the Group policies" are also used in the policy.

2. Policy implementation objectives

2.1. Ensure the confidentiality, integrity, authenticity, and accessibility of the Group's information.

2.2. In accordance with the highest information security standards, implement and develop an ISMS that ensures a secure and reliable information and cyber environment for the Companies, contributing to the achievement of the Group's strategic objectives.

2.3. Implement the National Cyber Security Strategy within the scope of competence and ensure compliance with applicable cyber security requirements.

2.4. Ensure the uninterrupted operation of the Companies and their resilience to information security incidents.

3. Internal and external factors

3.1. The ISMS is developed taking into account the directions set out in the Group's strategy and external and internal factors relevant to the Group's ISMS.

3.2. Internal factors relevant to the Group's ISMS:

3.2.1. The Group operates at national and international level (implementing projects important for national security, European projects, and ensuring compliance with common requirements);

3.2.2. The security and reliability of the Company's information systems is ensured by assessing and managing the risks posed by suppliers. The Group's energy transmission operators ensure the security and reliability of dispatch control based on their own information technology infrastructure (communications, data centres that are managed and developed);

3.2.3. The internal stakeholders are the Ministry of Energy of the Republic of Lithuania, the shareholders of the Companies, the Companies, the Management, and the Employees.

3.3. **External factors significant to the ISMS of the Group:**

3.3.1. LITGRID AB, AB Amber Grid, Energy cells UAB, in accordance with the Republic of Lithuania Law on the Protection of Objects Important to National Security, manages infrastructure that is important to national security and, together with EPSO-G, are recognized as second-category companies important for ensuring national security, and, in accordance with the provisions of the Republic of Lithuania Law on Cyber Security, are included in the register of essential cyber security entities in Lithuania;

3.3.2. The external stakeholders are the National Cyber Security Centre, Ministry of National Defence of the Republic of Lithuania, the Ministry of National Defence of the Republic of Lithuania, suppliers, energy companies, residents of the Republic of Lithuania, European Network of Transmission System Operators for Electricity and Gas, and other partners;

3.3.3. The Group performs actions in the field of information security in cooperation with and using the services provided by the National Cyber Security Centre, and in specific circumstances – with the Lithuanian police and the State Data Protection Inspectorate.

4. Basic principles of information security

4.1. **Confidentiality** – Sensitive information is not accessible or available to unauthorized persons or automated processes

4.2. **Integrity and authenticity** – the Group information is protected from accidental or unauthorized alteration or destruction, is accurate, reliable, and comes from a verified source.

4.3. **Availability** – the Group information is available when needed.

4.4. **Risk management** – The basis for the Group's information security management is determined by the proportionality, effectiveness, and continuous improvement of the measures applied. Information security risk assessment is performed on an ongoing basis, but at least once a year or when there is a significant change in the nature of the Company's activities, organisational structure, technological or threat environment, including the assessment of threats to national security, legal regulation, as well as after a major cyber incident. Information security risk management, assessment, and analysis methods are applied in accordance with the risk management policy and methodology of the UAB EPSO-G Group of Companies, the requirements of the Law on Cyber Security, and other relevant legislation.

4.5. **"Necessary for work" ("need to know")** – Confidential information and/or access to it shall be provided to persons only to the extent necessary for the performance of specific work and other functions related to the Group or the Company, obligations under the Company's transactions, or duties provided for in the legal acts of the Republic of Lithuania.

4.6. **"Least privileged access" –** access to Sensitive Information is granted with the least privileges (e.g., editing, copying, forwarding, etc.), that are sufficient to perform specific work and other functions related to the Group or the Company, obligations under the Companies' transactions or duties provided for in the legal acts of the Republic of Lithuania.

4.7. **The planning and implementation of measures is coordinated at the Group level** in order to identify common initiatives for the Companies and avoid duplication of functions and administrative activities, as well as to leverage the strengths of the Companies by sharing experience and expertise.

4.8. **Information security measures** are determined based on the security needs of each company (e.g., risk appetite, internal and external factors). Companies with the highest information security needs apply and implement cyber security risk management measures that meet the highest standards and best practices.

4.9. **Information security program** – a form of information security activity planning and management applied in companies, which includes the assessment of information security risks, compliance, and function maturity, as well as the definition of objectives and measures for a 3-year period.

4.10. **The effectiveness of ISMS activities is measured by indicators** – indicators are provided and monitored at the Group level, therefore the Group uses standardized or unified indicators ensuring security tools and processes.

4.11. **ISMS regulated at the Group level** – the essential internal legal acts implementing the Policy are managed, developed, and coordinated at the Group level. In order to make information security an integral part of daily activities, priority is given to integrating specific information security practices into the internal legislation of the relevant activities.

4.12. **Each Employee is directly involved in the implementation of the ISMS**. Employees are provided with the necessary knowledge through ongoing training and exercises, depending on the Employee‘s role in information security.

5. Compliance requirements

5.1. Information security in the Group is organised in accordance with the requirements set forth in the Law on Cyber Security and other Lithuanian and European legislation, as well as in accordance with the requirements set forth in the Companies‘ transactions applicable to the Companies.

5.2. A detailed list of legal acts regulating information security is provided and regularly updated in the Description of Information Security Procedure of EPSO-G Group of Companies.

5.3. Information security compliance is verified by internal and external audits, to the extent and frequency specified in the Description of Information Security Procedure of EPSO-G Group of Companies.

6. Application of standards

6.1. The complexity and optimality of information security management in the Group is ensured by implementing and continuously improving ISMS that complies with the requirements of the ISO/IEC 27001 standard.

6.2. The ISMS of the companies, which are subject to the highest level of information security requirement, is confirmed by the valid ISO/IEC 27001 certificate. The scope of certification covers the essential processes of each company: LITGRID AB – operations of the electricity transmission system operator, AB Amber Grid – operations of the natural gas transmission operator, Energy cells, UAB – operations of the designated storage system operator.

7. Duties and responsibilities

7.1. EPSO-G Board	7.1.1.	Approves this Policy, establishes the directions, objectives, goals, and principles of information security within the Group.
7.2. Management	7.2.1.	Undertakes to implement organisational and technical measures to ensure business continuity, information security compliance, and risk management, and to allocate the necessary resources to prevent business disruption due to a breach of the integrity, authenticity, availability, or confidentiality of the Group's information.
	7.2.2.	Once a year, reviews the ISMS effectiveness Management report and provides instructions and recommendations to ensure the implementation, suitability, effectiveness, and continuous improvement of the ISMS;
	7.2.3.	Ensures that Employees responsible for Information Security have the necessary means to perform their duties.
7.3. Managers at all levels	7.3.1.	Implements information security requirements, identifies and allocates the necessary resources within the scope of responsibility of their department and/or function and/or functional area.
	7.3.2.	Promotes a culture of information security and ensures that directly subordinate Employees are familiar with the Policy and the internal legal acts implementing it, understand the requirements and risks of non-compliance.
7.4. Information Security Manager of the Group	7.4.1.	On the basis of a management consulting agreement, performs the duties and functions of the Group's cyber security manager as set out in the Law on Cyber Security, and performs other functions assigned to the cyber security manager in legal acts regulating cyber security.
	7.4.2.	Formulates the Information Security Policy and monitors its implementation.
	7.4.3.	Prepares and, within the limits of their responsibility, approves Group-level information security governance documents and reviews them.
	7.4.4.	Coordinates information security planning activities between the Companies.
	7.4.5.	Participates in the management of Group information security incidents and events.
7.5. Information Security Manager of the Companies	7.5.1.	The Companies have appointed network and information system (all) security officers and perform the duties and functions of security officers as set out in the Law on Cyber Security. Ensures that the Company complies with the requirements set forth in the Law on Cyber Security, properly manages risks and incidents, and performs other functions set forth in the legal acts regulating cybersecurity.
	7.5.2.	Assesses, plans, implements, and controls information security.

	7.5.3. Implements the Policy and organises the implementation of the measures provided for in the legislation implementing it and risk management measures. 7.5.4. Prepares and updates Company-level ISVS documents and business continuity plans, and submits proposals for amendments to the Policy and Group-level internal legal acts implementing it to the Information Security Manager of the Group. 7.5.5. Manages information security incidents and events. 7.5.6. Identifies employees who have a specific information security role within the Companies and ensures that their knowledge and skills meet the requirements of their role and that they are adequately informed of any changes necessary to perform their role-related responsibilities. 7.5.7. In the first quarter of each year, prepares and submits to the Management a report on the effectiveness of the ISMS, agreed with the Information Security Manager of the Group, about: the implementation of objectives and actions identified in previous ISMS reviews, changes in the internal and external issues related to ISMS, the effectiveness of information security, and trends regarding non-compliance, corrective actions, monitoring and measurement, and audit (if any) results, feedback from stakeholders, risk assessment results, the status of the measures plan, and opportunities for continuous improvement.
7.6. Information Asset Managers (Owners)	7.6.1. Assigns the Company information and Information Assets to designated security classification categories, determines security requirements, and manages risks of and access to the Information Assets.
7.7. Employees	7.7.1. Comply with the requirements set forth in the Policy and the internal legal acts implementing it. 7.7.2. Use the information security measures provided by the Company and, within the limits of their responsibility, protect the Company's Information Assets from breaches of confidentiality, availability, authenticity, and integrity (e.g., unauthorized access, disclosure, modification, destruction). 7.7.3. Immediately inform the Company or the Information Security Manager of the Group of any detected or imminent Information Security incidents and violations of the Policy or other internal legal acts, as well as other divisions of the Companies, as established in the internal legal acts. 7.7.4. Ensure that contracts with third parties include the information security requirements applicable to third parties, as set out in the documents implementing the Policy, and liability for failure to comply with them. 7.7.5. attend cyber security training and participate in exercises pursuant to the procedure established by the head of the National Cyber Security Centre and in the Company.

7.8. The detailed responsibilities of the Management, Information Security Managers, and other employees are specified in the Group's internal legal acts implementing the Policy.

8. Final provisions

8.1. The Policy shall be reviewed and updated as necessary at least once a year or when significant changes occur (changes in the Group's structure, legal acts, after the occurrence of incidents, etc.). No later than within 5 working days from the date of approval and/or amendment of the Policy, the Information Security Managers of the Companies shall submit the title of the document, the date of approval, and the registration number via the information system of the National Cyber Security Centre.

8.2. Familiarization with the Policy shall be carried out in accordance with the procedure established in the internal legal acts of the Companies.